

Remarks

Applicants thank the Examiner for his careful consideration of the application.

Claims 9 – 16 and 18 – 23 are pending in the application.

Claim Rejections – 35 USC § 103

The Examiner rejected claims 9, 10, 13 – 15, 20, and 22 under 35 USC § 103(a) as being unpatentable over Spicer et al. (US Patent No. 7,007,093) (“Spicer”) in view of Harsch et al. (US Patent No. 7,088,698) (“Harsch”). Applicants respectfully traverse these rejections.

In claim 9, Applicants recite a method of accessing an internal network device on a protected network that includes a security device. The method includes storing data addressed to the internal network device in an external proxy server and maintaining a proxy agent on the protected network. The proxy agent polls the external proxy server for data addressed to the internal network device, forwards to the internal network device any data on the external proxy server and addressed to the internal network device, and forwards to the external proxy server any data addressed to an external device in communication with the external proxy server. Polling the external proxy server includes connecting to the external proxy server to check for pending traffic, receiving a stream of spurious bytes from the external proxy server if there is nothing pending for the internal network device, and receiving data from the external proxy server when the external proxy server has received data from a client.

The Examiner should withdraw the rejection to claim 9, as the Examiner has not made a prima facie case of obviousness. Specifically, the Examiner has not shown that the combination of references teaches that the proxy agent receives a stream of spurious bytes from the external proxy server if there is nothing pending for the internal network device. The stream of spurious bytes is a stream of false or misleading data. It is not a keep-alive message. The Examiner presents two arguments as to why the keep-alive method disclosed in Harsch is indistinguishable from Applicants’ spurious bytes. First, the Examiner argues that Applicants simply claim sending a stream of spurious bytes from the external proxy

server to the agent and not an intervening device for performing analysis. Second, the Examiner argues that Applicants' claim that a security device could detect the keep-alive messages is not based upon factual evidence. The first argument is irrelevant and the second is incorrect.

First, the Examiner asserts that Applicants do not refer to the security device when reciting the spurious bytes. Yes, the flow of spurious bytes is from the server to the agent. But these bytes, like all the data transferred, have to pass through the security device on their way to the agent. Stating that they pass through the security device seems superfluous. The reason Applicants send the spurious bytes is to fool the security device, but adding the purpose does not appear to be necessary. Applicants would be happy to explicitly add the reasoning if that will make a difference, but in Applicants' representative's experience, adding reasons or purposes to a claim has not affected whether a claim is allowable or not. The simple act of using spurious bytes rather than traditional keep-alive methods is in and of itself a patentable distinction over the combination of Harsch and Spicer as Applicants argue in response to the Examiner's second argument.

Second, the Examiner asserts that Applicants' have not produced evidence that the security device in Harsch would detect the keep-alive messages and that Applicants have failed to sufficiently characterize spurious bytes. Spurious bytes are self-explanatory. They are false and misleading data packets. They are not keep-alive messages sent to a security device essentially saying "I'm still here, please stay open." The reason why the spurious bytes are harder to detect is that they look like normal traffic where keep-alive packets do not. Keep-alive packets can be recognized easily, and the connection closed. Inspection of network packets by "stateful" firewalls is routine and widely deployed in the industry. These firewalls allow, disallow, and close connections based on knowledge of the connection state, which they maintain by inspecting incoming and outgoing traffic on a per-connection basis. For example, they are able to refuse a packet claiming to be a response, if their own record of the connection state indicates no corresponding preceding request. These stateful firewalls have been deployed since at least 1994 (Cheswick, Bellovin, and Rubin: "Internet Firewalls: Repelling the Wily Hacker", Addison-Wesley, 1994). Even if no existing security

device inspected packets to close connections not actually being used, it is easy to show why such devices might want to do so. The security devices do not want to keep connections alive if they are not actually being used; the connections use resources that others might use, and having them open invites external attack. Claim 9 recites a method that makes enforcement of such decisions harder for security devices by disguising traffic passing through them. Applicants designed the embodiment recited in claim 9 precisely because of problems that arose with stateful firewalls.

For each of the foregoing reasons, claim 9 is allowable over the combination of Spicer and Harsch.

The Examiner should allow claims 10, 13 – 15, 20, and 22 if claim 9 is allowed as claims 10, 13 – 15, 20, and 22 depend from claim 9.

The Examiner rejected claims 11, 12, 16, 18 – 21, and 23 under 35 USC § 103(a) as being unpatentable over Spicer in view of Harsch, and in further view of Grantges Jr. et al (US Patent No. 6,510,464) ("Grantges"). Applicants respectfully traverse these rejections. Claims 11, 12, 16, 18 – 21, and 23 all depend from claim 9. Applicants have already argued that the disclosure of Harsch does not disclose the use of "spurious bytes" to keep a connection open. As the Examiner has not identified this limitation in Grantges either, the Examiner has not established that the combination of Spicer, Harsch, and Grantges includes all the limitations of claim 9. Therefore, the Examiner should allow claims 11, 12, 16, 18 – 21, and 23 if claim 9 is allowed as claims 11, 12, 16, 18 – 21, and 23 depend from claim 9.

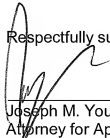
Conclusion

No additional fee is believed to be required for this amendment. However, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Application No. 09/845,104

A telephone interview is respectfully requested at the number listed below prior to any further Office Action, i.e., if the Examiner has any remaining questions or issues to address after this paper. The undersigned will be happy to discuss any further Examiner-proposed amendments as may be appropriate.

Respectfully submitted,



Joseph M. Young
Attorney for Applicants
Registration No. 45,248
Telephone (503) 685-4229
May 30, 2007

JMY/rjh